*Attaque réelle de *Troyens**

Case study :

Comment réagir lors d'une attaque de ***Troyens*** sur mon PC ? Est-ce que vous ne vous êtes pas déjà posés cette question ?

Pour les PC protégés d'un **anti-virus** et **Firewall**, pas de problèmes. Je vous montrerais maintenant comment faire en me basant sur un exemple pratique.

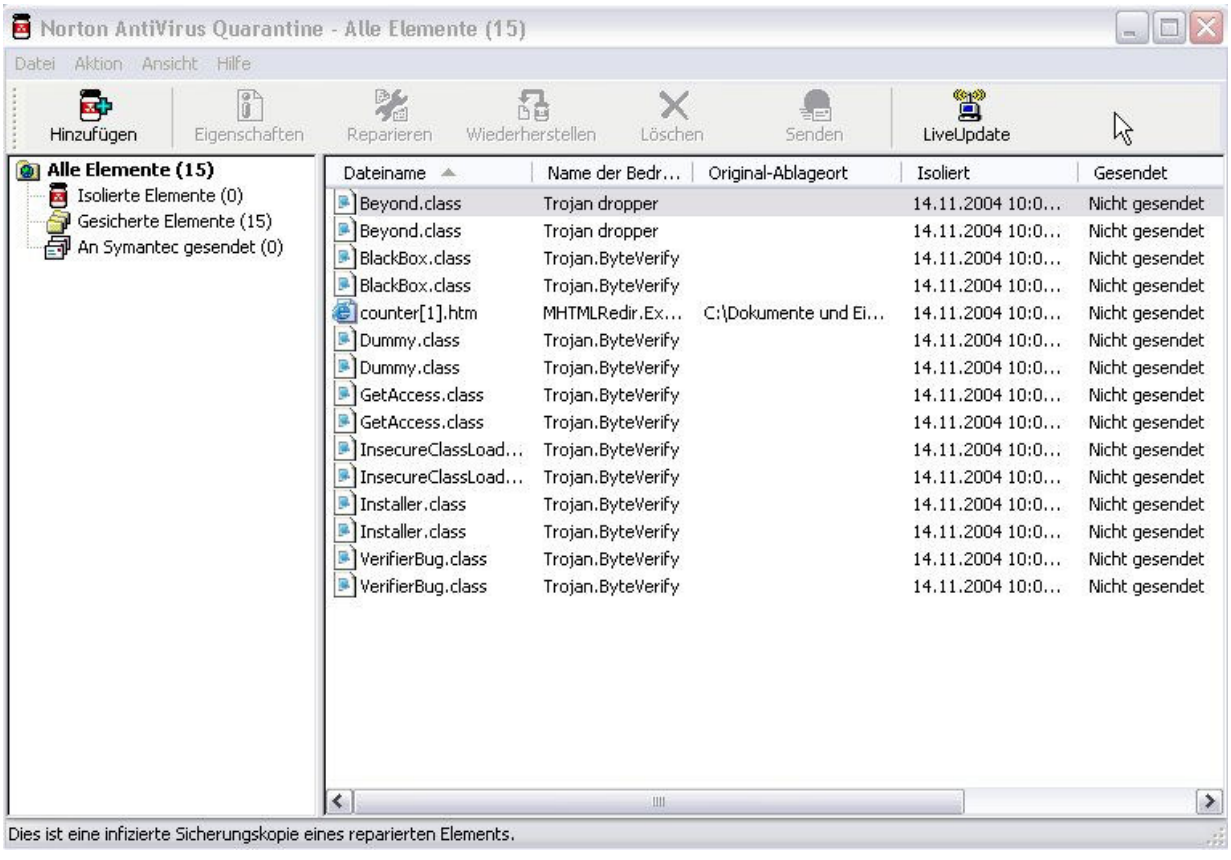
Pour ceux qui n'ont pas installé de logiciels de protection, ils ne sont apercevront même pas de ces attaques et les Troyens s'installeront sur leur PC !

Leur PC deviendra un ***PC ZOMBIE*** !

Je me suis payé le luxe d'aller chercher des* *Troyens sur Internet pour écrire ce tutoriel. Eh bien, croyez moi, c'est très facile d'en trouver et beaucoup plus facile que je m'imaginais ! (**Pas plus de cinq minutes !**)

Il suffit de scruter la ***Toile* (Internet**) en visitant des sites à caractère ***xxx*** et le fait simple de cliquer sur un lien et ou bien de visiter un site ***xxx*** quelconque pour attraper ces bestioles informatiques.
Quand vous visitez des sites d'échange de fichiers P2P, c'est pareil. Une étude a démontré que +/- 45% des fichiers téléchargés étaient contaminés.

Voyez vous-même la figure ci-dessous pour voir ***ce qui peut se passer en cliquant simplement sur un lien (Link) d'un certain site Internet, sans avoir installé des logiciels de sécurité.***



En visitant un seul site Internet, quinze (15) ***Troyens*** ont attaqué mon PC simultanément ! Heureusement que mon PC était protégé par ***Norton Internet Security*** ! Sinon, ***bonjour les dégâts*** !

Mon anti-virus avait très bien intercepté ces bestioles informatiques et les avait bloqué et mis en quarantaine. Ils sont enfermés dans le dossier ***quarantaine*** de mon anti-virus ***Norton Internet Security*** et ne sont plus nuisibles !

Nous allons examiner maintenant quelle sorte de ***malware*** (virus, vers, troyens, dialer, etc.) voulait envahir (attaquer) notre PC.
Pour ceci nous prenons recours à la base de données de chez **SYMANTEC**, fabricant de ***NORTON INTERNET SECURITY***.

Voici la liste des ***Troyens*** attrapés et mise en quarantaine par **NORTON INTERNET SECURITY** :

Beyond.class

Blackbox.class

Dummy.class

GetAccess.class

Insecure.ClassLoad

Installer.class

VerifierBug.class

MHTMLRedir.Ex

Cette liste ci-dessus représente les ***Troyens* Trojan.ByteVerify et Trojan.dropper**

Voyez ci-dessous la description de **SYMANTEC** de ces bestioles informatiques :

Trojan.ByteVerify is a Trojan Horse that exploits the vulnerability described in Microsoft Security Bulletin MS03-011 and could provide a hacker the ability to run arbitrary code on an infected system.

http://securityresponse.symantec.com/avcenter/venc/data/trojan.byteverify.html

Trojan dropper is a Trojan horse that drops Trojan horses or Backdoor Trojans onto an infected computer

http://securityresponse.symantec.com/avcenter/venc/data/trojan.dropper.html

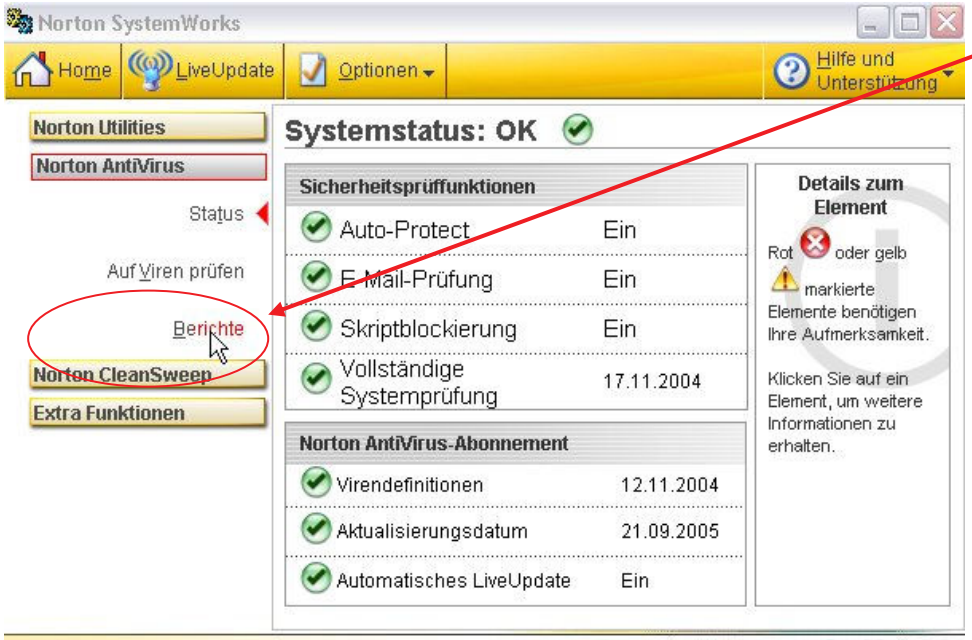
En faisant la traduction résumant les explications ci-dessus, les ***Troyens*** qui attaquaient mon PC voulaient introduire un programme ***backdoor***.

Un programme ***backdoor*** est un programme contenant un ***keylogger*** et qui ouvre les ports de communication vers l'extérieur.

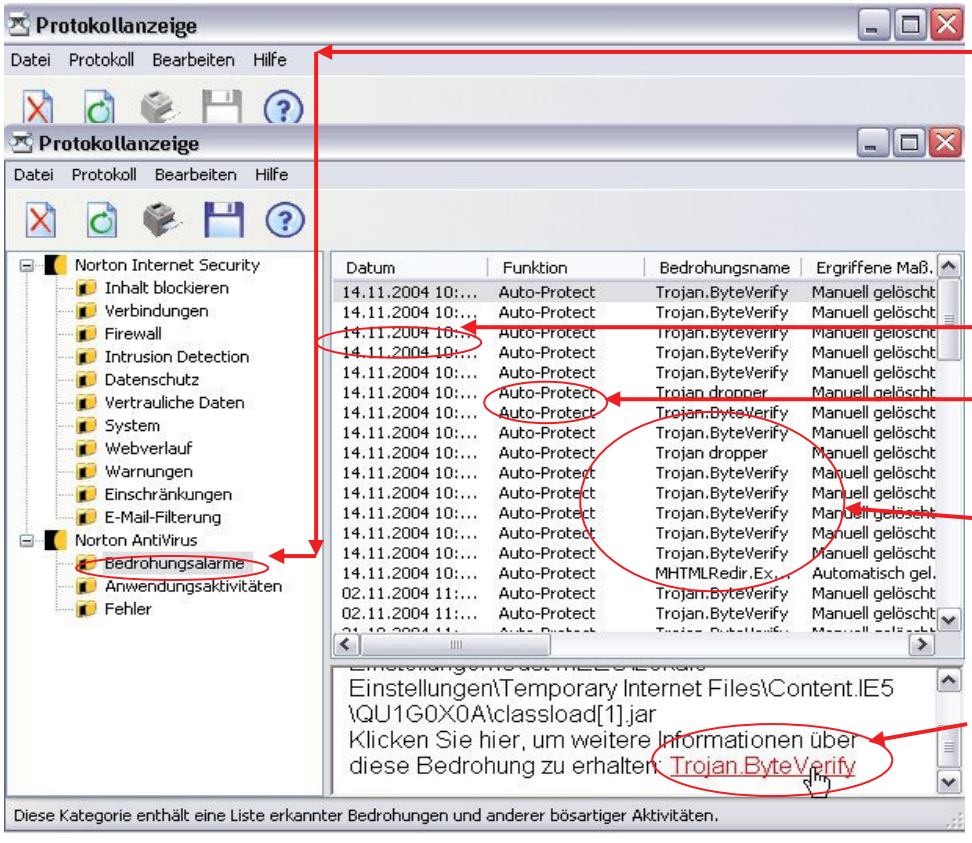
Sans ma protection, ces bestioles informatiques auraient volés mes mots de passe, données bancaires, mes codes d'accès et auraient envoyé ces informations envers leur créateur. Celui-ci aurait pu alors téléguider mon PC à mon insu sans que je m'en aperçoive !

Comment est-ce que j'ai trouvé le nom de ces bestioles informatiques ?

Pour trouver le nom des Troyens qui ont attaqués mon PC, il suffit d'ouvrir notre logiciel (programme) anti-virus, qui lui enregistre toutes attaque et qui fait un protocole détaillé.



Pour ceci nous cliquons sur *Rapports* (*Berichte*), ce qui nous ouvre une autre boîte de dialogue.



Nous cliquons ensuite sur *Menaces* (Bedrohungsalarme)

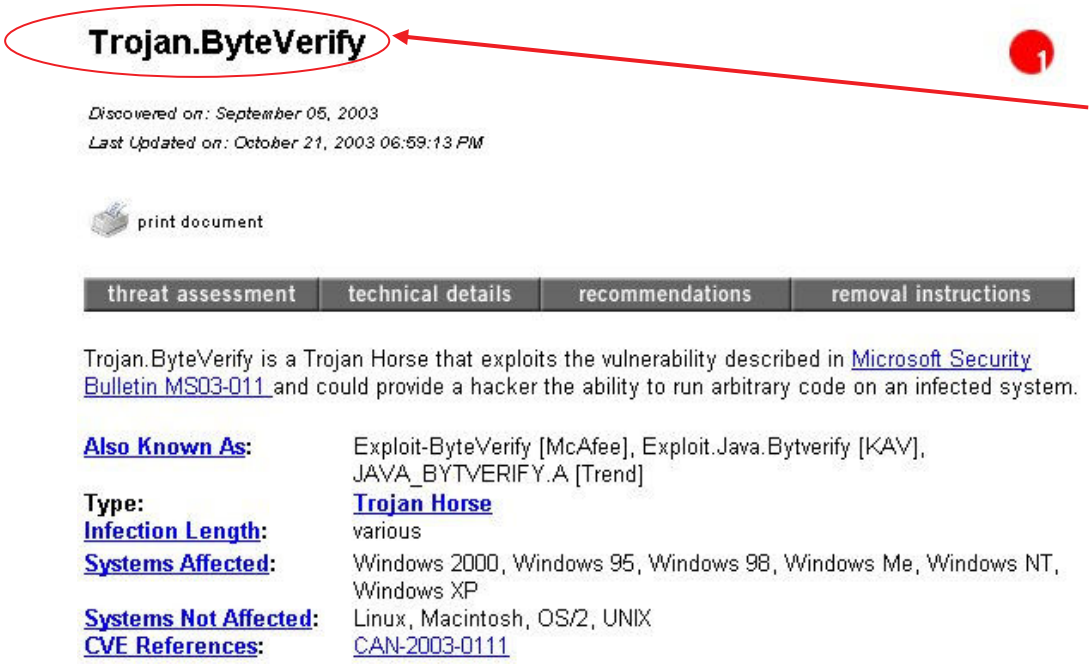
Dans la partie droite nous voyons maintenant les informations suivantes:

Date et heure de l'attaque

Le statut de notre anti-virus

Le nom de la malware

Les informations sur la malware. En cliquant ce lien, nous serons digérés sur le site de **SYMANTEC**



Maintenant nous recevons toutes les informations sur cette malware.

Maintenant que nous savons ce que c'est un ***Troyen*** et quels dégâts qu'il peut provoquer, vous vous posez certainement la question

Comment nous protéger?

1. Pour ne laisser entrer un ***Troyen*** sur notre PC, ni le laisser sortir de notre PC il nous faut installer un ***Firewall*** !

2. Comme protection supplémentaire, qui éradique les ***Troyens*** déjà présents sur notre PC et qui nous protège aussi contre les attaques des ***Troyens*** et des ***Dialer***, nous devons installer un logiciel ***anti-malware*** tel que ***a2*** de **EMSISOFT.**

Un Firewall très performant et aussi GRATUIT (FREEWARE) est ZONEALARM de ZONELABS dont voici le lien :

http://www.zonelabs.com

Fonctions des logiciels (programmes) discutés :

Le ***Firewall*** nous protège contre les données entrantes et sortantes non désirées. Si jamais il y aurait un *Troyen* installé sur notre PC, le *Firewall* bloquerait sa connexion vers l'extérieur, mais il serait toujours résident sur le disque dur de notre PC.

Pour éradiquer maintenant ce ***Troyen*** et aussi nous protéger contre ce ***malware***, il nous faut installer un logiciel (programme) ***anti-troyen*** ou ***anti-malware***.

Je vous conseille ***a squared (a2)*** de chez **EMSISOFT.** C'est un logiciel (programme) multi langues, qui nous protège contre les ***malware*** (virus, vers, troyens, dialer, etc.).

Voici l'adresse URL pour le télécharger (download) :

http://www.emsisoft.com

Copyright © by Gust MEES (LU) 2004 / 5 - 6 Attaque réelle de *Troyens*

Pour le téléchargement, l'installation, ainsi que l'utilisation de ***a2*** veuillez suivre mes conseils dans mon tutoriel (Cours gratuit online) à l'adresse suivante (Format PDF) :

http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=Tutoriel_12.11.2004..pdf&startid=3402&id_classeur=803

Le logiciel (programme) ***a squared (a2)*** est **à voir comme un complément** à l'anti-virus et au ***Firewall*** et c'est un logiciel très performant et simple dans son utilisation. Personnellement je l'utilise déjà plus d'un an et très content avec.

a² Personal est le successeur des produits "Anti-Trojan 5.5" et "ANTS 2.1" Scanner de Trojans.

a² Free
sans "Gardien d'arrière-plan"

a² Free c'est l'alternative gratuite de a² Personal. Nettoyer votre PC des Malwares existant. a² Free ne contient pas de Gardien d'arrière-plan, qui peut si une nouvelle infection il y a, empêcher celle-ci.

Il existe en deux versions, une version Freeware et une version payante. **La version payante coûte 29,95 €.**

a² Personal est un Malware Scanner et Destructeur de Malware de nouvelle génération. a² reconnaît les chevaux de Troie, Backdoors, Virus, Dialer, Spywares et tous les programmes dangereux avec lesquels un intrus pourrait endommager votre PC, ou voler vos données privées. Le Gardien d'arrière-plan protége votre ordinateur en bloquant les malware avant qu'ils ne deviennent actifs.

Je vous conseille aussi de visiter mon site Internet sur la Sécurité PC&Internet à l'adresse suivante :

http://www.webwizardbiz.com/tutorials/guidesecurite/

Le logiciel ***a squared (a2)*** tourne en arrière-plan comme l'anti-virus et vous pouvez travailler avec votre PC en même temps que ces logiciels tournent.

Un peu plus lent, mais quand même !

Pourquoi certains sites Internet sont-ils contaminés ?

C'est bien évidemment dans un but commercial. Comme la majorité des **internautes** (utilisateurs d'Internet) n'est pas soucieux des problèmes de sécurité et que certains s'en foutent carrément, ils sont une proie facile pour les truands et escrocs.

La plupart des internautes visitent les sites Internet ***xxx***, donc à **contenu pornographique**, par pure curiosité. Cette curiosité peut leur coûter cher sans protection anti-virus et sans firewall.

Car pas mal de sites Internet porno veulent exploiter cette **naïveté** des internautes ! Et croyez moi, ils gagnent bel et bien leur pain avec **(€, $, £)** !

Ces sites Internet à contenu ***xxx*** sont à comparer avec **le milieu dit *rouge*** dans les villes dans la proximité des stations des chemins de fer. Ce milieu rouge est à considérer comme dangereux car pas mal d'escrocs essaient de profiter de la naïveté des visiteurs de ces quartiers.

En plus d'une attaque de ***Troyens***, nous pouvons aussi attraper un ***Dialer***. Un seul ***clic*** avec la souris sur un lien ou lien d'image (**bannière**) suffit que les **internautes** (utilisateurs d'Internet) soient redirigés envers un site payant ou ils téléchargent (**download**) un **plug-in** pour visionner le contenu du dit site Internet.

Ce *plug-in* est au fait un *Dialer*, une connexion surtaxée ! Ces connexions surtaxées peuvent varier de 5 €/minute à 60 € / minute et ou 50 € par clic ! Bonjour les dégâts !

Pour savoir plus sur les ***Dialer***, veuillez visiter mon tutoriel à l'adresse suivante :

http://www.webwizardbiz.com/tutorials/dialer/

25349

€